UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information that is Stored at Premises Controlled by Google

Case No. 21 MJ 209

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A (incorporated by reference). This court has authority to issue this warrant under 18 U.S.C. §§ 2703 (c)(1)(A) and 2711(3)(A).

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B (incorporated by reference).

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 922(i)	Knowingly transporting stolen firearm
18 U.S.C. § 922(j)	Knowing possession of a stolen firearm
18 U.S.C. § 922(u)	Theft of firearm from federal firearms licensee

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

BRADLEY KURTZWEIL Digitally signed by BRADLEY KURTZWEIL Date: 2021.10.19 09:11:48 -05'00'

Applicant's signature

ATF SA Brad Kurtzweil

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 10/19/2021

William E. Duffin

Judge's signature

City and state: Milwaukee, Wisconsin

Hon. William E. Duffin, Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Bradley Kurtzweil, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search information that is stored at premises controlled by Google, an electronic communication service and remote computing service provider headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government the information further described in Attachment B.I. The government will then review that information and seize the information that is further described in Attachment B.II.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), currently assigned to the Milwaukee Field Office. I have been so employed since March 2020. My duties as a Special Agent with ATF include investigating alleged violations of the federal firearms, explosives, and arson statutes. I have completed approximately 26 weeks of training (approximately 1000 hours) at the Federal Law Enforcement Training Center (Glynco, Georgia), as well as the ATF National Academy. During my time as an ATF Special Agent, I have investigated cases involving firearms, narcotics, gangs, arson, and fraud.

3. Prior to my employment with the ATF, I was a sworn Police Officer in the State of Illinois from March 2011 to March 2020. I served as a patrol officer and evidence technician. I completed 12 Weeks (approximately 480 hours) of basic training at the Illinois

State Police Academy from April 2011 to June 2011. I later attended approximately 520 hours of additional training throughout my time as a police officer, in areas including: Evidence collection, interview/interrogation, arson and explosives, gang investigations and drug investigations.

4. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, and through information provided to me by other law enforcement officers, who have provided information to me during the course of their official duties and whom I consider to be truthful and reliable.

5. I submit this affidavit for the limited purpose of demonstrating sufficient probable cause for the requested warrant. It does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the information described below, there is probable cause to believe that unknown persons have violated Title 18, United States Code, Sections 922(i), 922(j), 922(u), and 924(m). There is also probable cause to search the information described in Attachment A for evidence of these crimes, further described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

8. Based on my training and experience, I know that cellular devices, such as mobile telephone(s), are wireless devices that enable their users to send or receive wire and/or electronic communications using the networks provided by cellular service providers. Using cellular networks, users of many cellular devices can send and receive communications over the Internet.

9. I also know that many devices, including but not limited to cellular devices, have the ability to connect to wireless Internet ("wi-fi") access points if the user enables wi-fi connectivity. These devices can, in such cases, enable their users to send or receive wire and/or electronic communications via the wi-fi network. A tablet such as an iPad is an example of a device that may not have cellular service but that could connect to the Internet via wi-fi. Wi-fi access points, such as those created through the use of a router and offered in places like homes, hotels, airports, and coffee shops, are identified by a service set identifier ("SSID") that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device's wi-fi settings.

10. Based on my training and experience, I also know that many devices, including many cellular and mobile devices, feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a device such as a cellular phone or tablet and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a device routinely scans its environment to identify Bluetooth devices, which emit beacons that can

be detected by devices within the Bluetooth device's transmission range, to which it might connect.

11. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the device can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the apps' operation.

12. Based on my training and experience, I know Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every device using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

13. In addition, based on my training and experience, I know that Google offers numerous apps and online-based services, including messaging and calling (*e.g.,* Gmail, Hangouts, Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage, and sharing (*e.g.*, Drive, Keep, Photos, and YouTube). Many of these services are accessible only to users who have signed into their Google accounts. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address (*e.g.*, example@gmail.com). Other services, such as Maps and YouTube, can be used with limited functionality without the user being signed into a Google account.

14. Based on my training and experience, I also know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user

has the ability to sign-in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be uploaded to Google and then synced across the various devices on which the subscriber may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices and Windows computers, among others.

15. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices.

16. According to my training and experience, as well as open-source materials published by Google, I know that Google offers accountholders a service called "Location History," which authorizes Google, when certain prerequisites are satisfied, to collect and retain a record of the locations where Google calculated a device to be based on information transmitted to Google by the device. That Location History is stored on Google servers, and it is associated with the Google account that is associated with the device. Each accountholder may view their Location History and may delete all or part of it at any time.

17. Based on my training and experience, I know that the location information collected by Google and stored within an account's Location History is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device. Google uses this information to calculate the device's estimated latitude and longitude, which varies in its accuracy depending on the source of the

data. Google records the margin of error for its calculation as to the location of a device as a meter radius, referred to by Google as a "maps display radius," for each latitude and longitude point.

18. Based on open-source materials published by Google and my training and experience, I know that Location History is not turned on by default. A Google accountholder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account in order for that usage to be recorded in Location History. A Google accountholder can also prevent additional Location History records from being created at any time by turning off the Location History setting for their Google account or by disabling location reporting for a particular device or Google application. When Location History is enabled, however, Google collects and retains location data for each device with Location Services enabled, associates it with the relevant Google account, and then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising. As noted above, the Google accountholder also has the ability to view and, if desired, delete some or all Location History entries at any time by logging into their Google account or by enabling auto-deletion of their Location History records older than a set number of months.

19. Location data, such as the location data in the possession of Google in the form of its users' Location Histories, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected and retained via the use of Google products as described above, devices that were likely in a particular geographic area during a particular

time frame and to determine which Google account(s) those devices are associated with. Among other things, this information can indicate that a Google accountholder was near a given location at a time relevant to the criminal investigation by showing that his/her device reported being there.

20. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provide clues to their identity, location, or illicit activities.

21. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (*i.e.,* session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device

that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

PROBABLE CAUSE

22. On October 9, 2021, at approximately 11:10 a.m., two men entered Ron's Gun Shop at N112W16340 Mequon Road, in Germantown, Wisconsin. One of them ("Suspect 1") was wearing jeans, with blue shorts or briefs visible underneath, a gray hooded sweatshirt, and had a yellow hat or wrap on his head. The other man ("Suspect 2") was wearing black pants, a black t-shirt with a large orange "V" and the numbers "9 9 9" on the back of the shirt, sunglasses, and a black camouflage wrap on his head. Both men had cell phones in their hands. Neither subject was wearing a mask or face covering.

23. Ron's Gun Shop is a federal firearms licensee. The store is equipped with a video surveillance system, which captured and stored footage of the events discussed herein.

24. After entering the store, Suspect 1 engaged a store employee who was on the phone in conversation. In doing so, Suspect 1 positioned himself so that Suspect 2 was not in the employee's line of sight. At the time of the theft, there were no other store employees or customers present in the business.

25. As Suspect 1 spoke with the store employee, video footage shows Suspect 2 reaching over a gun case. He slid the unlocked door open, and removed two handguns (a Ruger Max-9, 9mm pistol bearing serial no. 350062131; and a Smith & Wesson M&P 9, 9mm pistol bearing serial number NKP8131) from the case. Suspect 2 then quickly concealed the handguns in the front of his waistband under his shirt, and slid the gun case door closed. Suspect 2 signaled Suspect 1 with a head nod and both left the shop on foot, running east from the shop location. (See Figure 1, 2 and 3 below).

Figure 1 (Suspect 1)

Figure 2 (Suspect 2)

Figure 3

26. The next day, on October 10, 2021, at approximately 6:25 p.m., two men entered the "Gun Library," located inside the Cabela's department store at 1 Cabela Way, in Richfield, Wisconsin. Cabela's is a federal firearms licensee. The store is equipped with a video surveillance system, which captured and stored footage of the events discussed herein.

27. Having viewed and compared the surveillance footage taken from both stores, it appears that the two men in the Cabela's "Gun Library" at 6:25 p.m. on October 10 were the same individuals who were at Ron's Gun Shop at around 11:10 a.m. the previous day as described above. More specifically, one of them was wearing jeans, with blue shorts or briefs visible underneath, a black tank top, and had an orange hat or warp on his head. In addition to the similarity in clothing, the man's height and build matched the depiction of Suspect 1. The second man was wearing black pants, a black t-shirt with a large orange "V" and the numbers "9 9 9" on the back of the shirt, sunglasses, and a black camouflage wrap on his head. In addition to the similarity in clothing, the man's height and build matched the depiction of Suspect 2. (See Figures 4, 5 and 6 below).

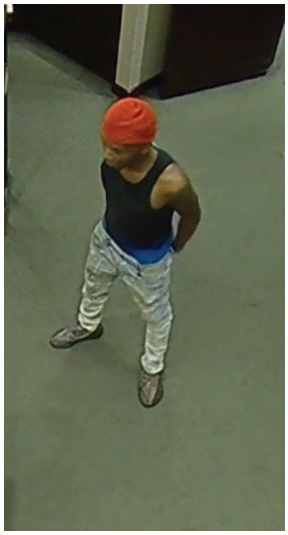


Figure 4 (Suspect 1)

Figure 5 (Suspect 2)

Figure 6

28. Aside from Suspect 1, Suspect 2, and store employee assisting them (all shown in Figure 6 above), there were no customers or employees present in the Cabela's "Gun Library" at the time.

29. The Cabela's employee opened a locked gun case and handed a firearm to Suspect 1. While Suspect 1 was examining the firearm, Suspect 2 squatted down in front of the now unlocked and open case and removed a firearm (Glock 41 pistol, .45 Caliber, Serial Number ZTC059). The store employee was momentarily distracted as he moved to close the case, and Suspect 2 concealed the Glock next to his right leg while turning away from the employee. He then hid the gun in his rear pants pocket and covered it with his shirt. Suspect 2 signaled Suspect 1 by tapping on his shoulder/arm. Suspect 2 then handed the gun in his hands back to the employee. Both suspects left the store and appeared to enter a vehicle in the store's parking lot. (This footage is somewhat obstructed by trees and other vehicles, and is also less clear due to the distance from the surveillance camera.)

30. Based on the foregoing, I submit that there is probable cause to search information that is currently in the possession of Google and that relates to the devices that reported being within the Target Locations described in Attachment A during the time periods described in Attachment A for evidence of the crime(s) under investigation. The information to be searched includes (1) identifiers of each device; (2) the location(s) reported by each device to Google and the associated timestamp; and (3) basic subscriber information for the Google account(s) associated with each device.

31. The proposed warrant sets forth a multi-step process whereby the government will obtain the information described above. Specifically, as described in Attachment B.I:

a. Using Location History data, Google will identify those devices that it calculated were or could have been (based on the associated margin of error for the estimated latitude/longitude point) within the Target Locations described in Attachment A during the time periods described in Attachment A. For each device, Google will provide an anonymized identifier, known as a Reverse Location Obfuscation Identifier ("RLOI"), that Google creates and assigns to devices for purposes of responding to this search warrant; Google will also provide each device's location coordinates along with the associated timestamp(s), margin(s) of error for the coordinates (*i.e,.* "maps display radius"), and source(s) from which the location data was derived (*e.g.*, GPS, wi-fi, bluetooth), if available. Google will not, in this step, provide the Google account identifiers (*e.g.,* example@gmail.com) associated with the devices or basic subscriber information for those accounts to the government.

b. The government will identify to Google the devices appearing on the list produced in step 1 for which it seeks the Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.

c. Google will then disclose to the government the Google account identifier associated with the devices identified by the government, along with basic subscriber information for those accounts.

32. This process furthers efficiency and privacy by allowing for the possibility that the government, upon reviewing contextual information for all devices identified by Google, may be able to determine that one or more devices associated with a Google account (and

the associated basic subscriber information) are likely to be of heightened evidentiary value and warrant further investigation before the records of other accounts in use in the area are disclosed to the government.

CONCLUSION

33. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c).

34. I further request that the Court direct Google to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property To Be Searched

This warrant is directed to Google LLC and applies to:

(1) Location History data, sourced from information including GPS data and information about visible wi-fi points and Bluetooth beacons transmitted from devices to Google, reflecting devices that Google calculated were or could have been (as indicated by margin of error, *i.e.,* "maps display radius") located within each of the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below ("Initial Search Parameters"); and

(2) Identifying information for Google Accounts associated with the responsive Location History data.

Initial Search Parameters

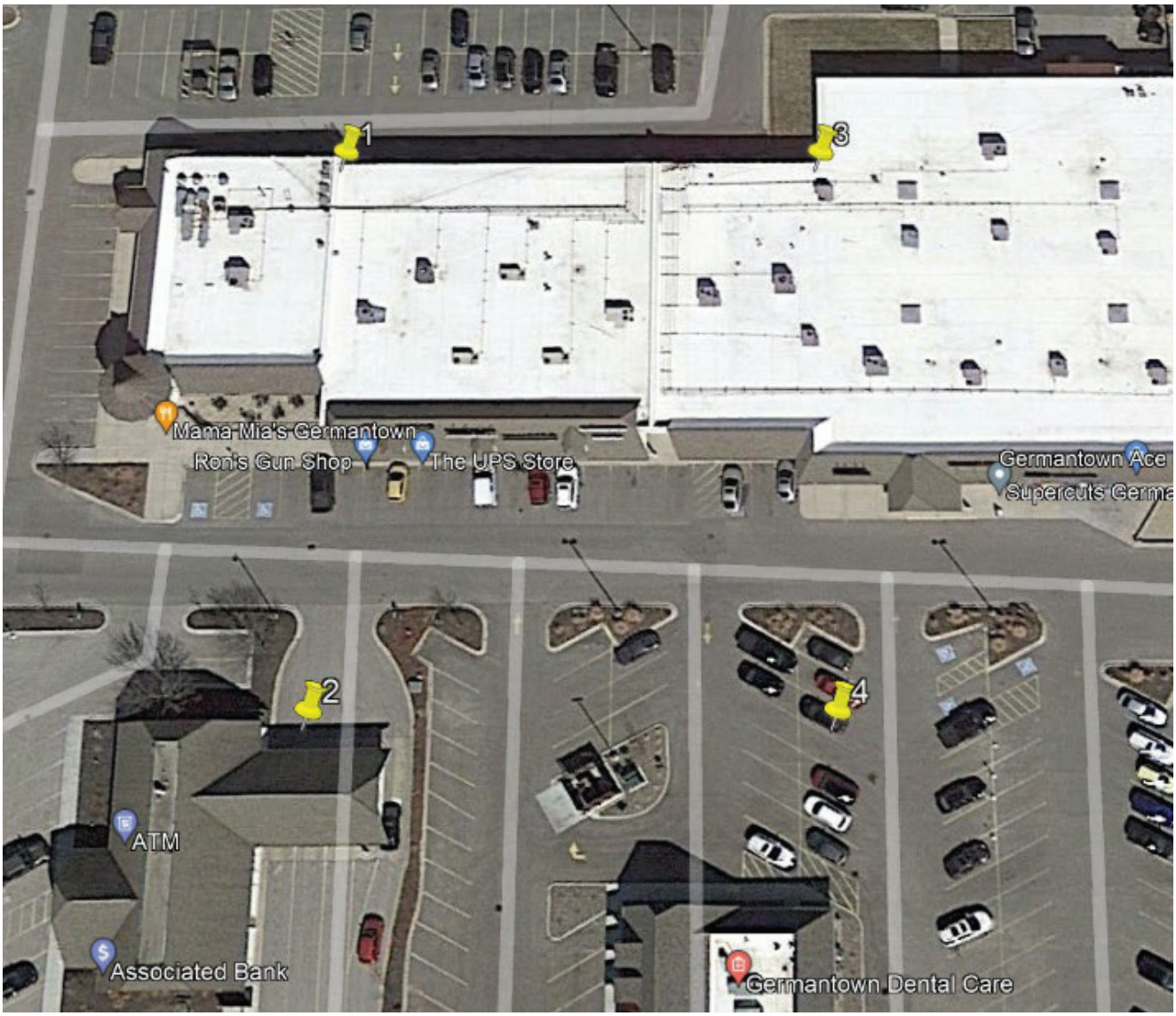
Search Parameter One

Date: October 9, 2021
Time Period: 11:05 a.m. to 11:15 a.m. (Central Daylight Time)
Target Location: A rectangular geographical area defined by the following latitude/longitude coordinates:

(1) 43.222233, -88.112147; (2) 43.221681, -88.112144;

(3) 43.222233, -88.111531; (4) 43.221681, -88.111522

Also approximately depicted in the following image:



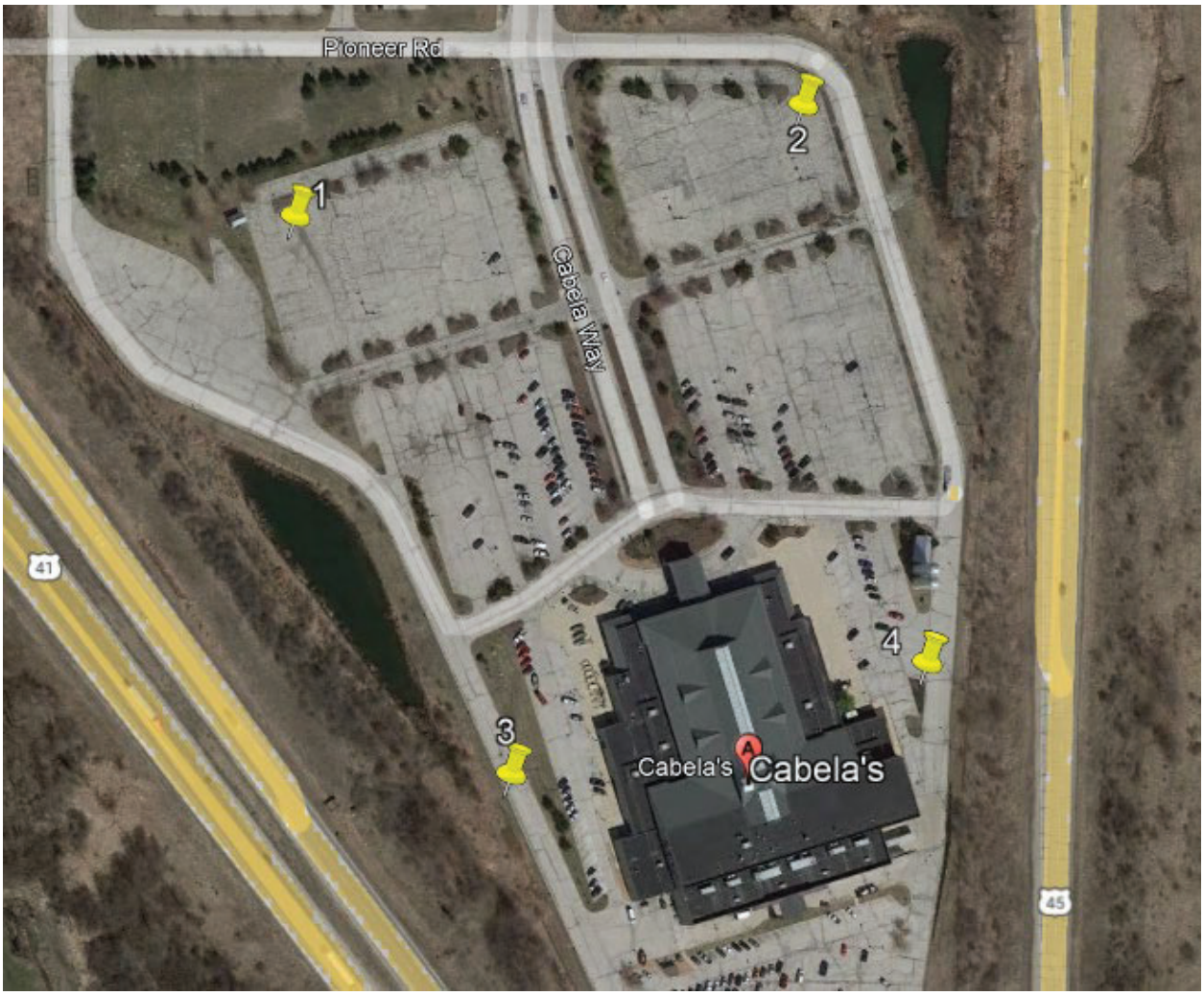
Search Parameter Two

Date: October 10, 2021
Time Period: 6:20 PM to 6:35 PM (Central Daylight Time)
Target Location: A four-sided geographical area defined by the following latitude/longitude coordinates:

(1) 43.280103, -88.190261; (2) 43.280517, -88.187658;

(3) 43.278019, -88.189156; (4) 43.278436, -88.187022

Also approximately depicted in the following image:



Google is further ordered to disclose the above information to the Government within 14 days of the issuance of this warrant.

ATTACHMENT B

Particular Items to Be Seized

I. Information to be disclosed by Google

The information described in Attachment A, via the following process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A. For each location point recorded within the Initial Search Parameters, and for each location point recorded outside the Initial Search Parameters where the margin of error (*i.e.*, "maps display radius") would permit the device to be located within the Initial Search Parameters, Google shall produce to the government information specifying the corresponding unique device ID, timestamp, location coordinates, display radius, and data source, if available (the "Device List").

2. The government shall review the Device List and identify to Google the devices about which it seeks to obtain Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.

3. Google shall disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Accounts associated with each device ID appearing on the Device List about which the government inquires.

II. Information to Be Seized

All information described above in Section I that constitutes evidence of violations of Title 18, United States Code, Sections 922(i), 922(j), 922(u), and 924(m), committed on October 9-10, 2021, involving unknown persons.